TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
11/10/2020

SUBJECT:
Critical Patches Issued for Microsoft Products, November 10, 2020

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
Google disclosed that CVE-2020-17087 has been actively being exploited in the wild which allows an attacker to escalate their privileges.

SYSTEMS AFFECTED:
- Microsoft Windows
- Microsoft Office and Microsoft Office Services and Web Apps
- Internet Explorer
- Microsoft Edge (EdgeHTML-based)
- Microsoft Edge (Chromium-based)
- ChakraCore
- Microsoft Exchange Server
- Microsoft Dynamics
- Microsoft Windows Codecs Library
- Azure Sphere
- Windows Defender
- Microsoft Teams
- Azure SDK
- Azure DevOps
- Visual Studio

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution.

A full list of all vulnerabilities can be found at the link below:
https://portal.msrc.microsoft.com/en-us/security-guidance

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches or appropriate mitigations provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack.
- Remind all users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Microsoft:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://msrc.microsoft.com/update-guide/releaseNote/2020-Nov

Google:
https://bugs.chromium.org/p/project-zero/issues/detail?id=2104